PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-142682

(43)Date of publication of application : 25.05.2001

(51)Int.Cl. G06F 7/58

(21)Application number : 11-323252

(22)Date of filing : 12.11.1999

(71)Applicant : SONY CORP

(72)Inventor : SHIBAIKE YUKO

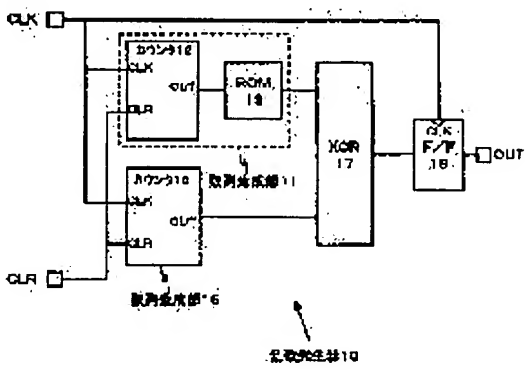
NODA TOSHIHARU

(54) RANDOM NUMBER GENERATOR AND RANDOM NUMBER GENERATING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To generate random numbers with long cycle at a low cost.

SOLUTION: This random number generator is provided with a first sequence generating part to generate a sequence with a first cycle, a second sequence generating part to generate a sequence with a second cycle and an arithmetic part to apply a prescribed arithmetic operation to the first and second sequences. The first sequence generating part outputs random numbers read, for example, from a random number table. The second sequence generating part is allowed to be a counter output to increment in stepped or other complicated forms which are not the counter output other than a normal counter output. The arithmetic part generates uniform random numbers without deviation by applying XOR and XNOR, etc., to the first and second sequences. Since the generated random numbers have the greatest common divisor of the first and second cycles as the cycles, their cycles are easily prolonged.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－142682
（P2001－142682A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全７頁）

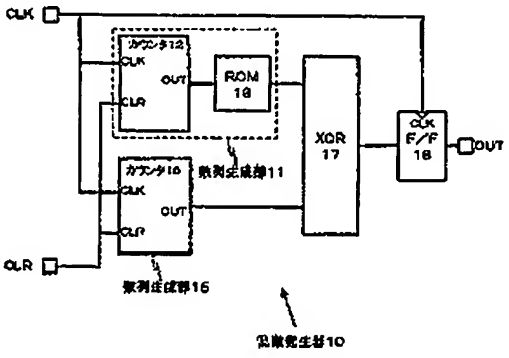
(21)出願番号　特願平11－323252

(22)出願日　平成11年11月12日(1999.11.12)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　芝池　優子
東京都品川区東五反田１丁目14番10号　株式会社ソニー木原研究所内
(72)発明者　野田　俊治
東京都品川区東五反田１丁目14番10号　株式会社ソニー木原研究所内
(74)代理人　100101801
弁理士　山田　英治　（外２名）

(54)【発明の名称】　乱数発生装置及び乱数発生方法

(57)【要約】
【課題】　長周期の乱数を低コストで発生する。
【解決手段】　乱数発生装置は、第１の周期を持つ数列を生成する第１の数列生成部と、第２の周期を持つ数列を生成する第２の数列生成部と、前記第１及び第２の数列に対して所定の演算を適用する演算部とを備える。第１の数列生成部は例えば乱数テーブルから読み出した乱数を出力する。第２の数列生成部は通常のカウンタ出力である他、階段状その他複雑な形式でインクリメントするカウンタ出力、カウンタ出力でない数列でよい。演算部は、第１及び第２の数列にＸＯＲやＸＮＯＲなどを適用して、偏りのない一様な乱数を生成する。生成された乱数は、第１及び第２の周期の最小公倍数を周期に持つので、容易に長周期化できる。



1

【特許請求の範囲】

【請求項１】第１の周期を持つ第１の数列を生成する第１の数列生成部と、

第２の周期を持つ第２の数列を生成する第２の数列生成部と、

前記第１及び第２の数列に対して所定の演算を適用する演算部と、

前記演算部の演算結果を乱数として出力する出力部と、を具備することを特徴とする乱数発生装置。

【請求項２】前記第１の数列生成部は、カウント値を逐次インクリメントするカウンタと、第１の周期を持つ乱数テーブルを含み、前記乱数テーブル中からカウント値に該当するエントリの乱数を出力することを特徴とする請求項１に記載の乱数発生装置。

【請求項３】前記第２の数列生成部は、０～（Ｎ－１）の数値の範囲を逐次インクリメントし、周期Ｎを有するカウンタであることを特徴とする請求項１に記載の乱数発生装置（但し、Ｎは１以上の整数）。

【請求項４】前記第２の数列生成部は、０～（Ｎ－１）の数値の範囲を階段状にインクリメントし、周期Ｎ×（Ｎ＋１）／２を有するカウンタであることを特徴とする請求項１に記載の乱数発生装置（但し、Ｎは１以上の整数）。

【請求項５】前記演算部は、前記第１及び第２の数列に対してＸＯＲ（排他的論理和）又はＸＮＯＲ（排他的否定論理和）などの排他的論理演算を適用することを特徴とする請求項１に記載の乱数発生装置。

【請求項６】前記第１及び第２の周期は互いに約数を持たないことを特徴とする請求項１に記載の乱数発生装置。

【請求項７】第１の周期を持つ第１の数列を生成するステップと、

第２の周期を持つ第２の数列を生成するステップと、

前記第１及び第２の数列に対して所定の演算を適用するステップと、

前記演算部の演算結果を乱数として出力するステップと、を具備することを特徴とする乱数発生方法。

【請求項８】前記第１の数列を生成するステップでは、第１の周期を持つ乱数テーブル中から、逐次インクリメントされるカウント値に該当するエントリの乱数を出力することを特徴とする請求項７に記載の乱数発生方法。

【請求項９】前記第２の数列を生成するステップでは、０～（Ｎ－１）の数値の範囲を逐次インクリメントして、周期Ｎを持つカウント値を生成することを特徴とする請求項７に記載の乱数発生方法（但し、Ｎは１以上の整数）。

【請求項１０】前記第２の数列を生成するステップでは、０～（Ｎ－１）の数値の範囲を階段状にインクリメントして、周期Ｎ×（Ｎ＋１）／２を有するカウント値を生成することを特徴とする請求項７に記載の乱数発生方法（但し、Ｎは１以上の整数）。

2

【請求項１１】前記所定の演算を適用するステップでは、前記第１及び第２の数列に対してＸＯＲ（排他的論理和）又はＸＮＯＲ（排他的否定論理和）などの排他的論理演算を適用することを特徴とする請求項７に記載の乱数発生方法。

【請求項１２】前記第１及び第２の周期は互いに約数を持たないことを特徴とする請求項７に記載の乱数発生方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無作為に選ばれた全く不規則な数字の列で構成される乱数を発生するための乱数発生装置及び乱数発生方法に係り、特に、長周期の乱数を発生することができる乱数発生装置及び乱数発生方法に関する。

【０００２】

【従来の技術】昨今の情報処理技術の進歩に伴い、各種のコンピュータ・システムが広汎に普及してきている。コンピュータ上では、テキスト、画像、音声などあらゆるデータをデジタル化して、各種の業務処理の支援・自動化が可能である。

【０００３】かかるコンピュータ処理の各局面においては、乱数、すなわち無作為に選ばれた全く不規則で偏りのない数字の列がしばしば利用される。例えば、データの暗号化や電子認証を行う際などに、各数値の間に相関性がなく、第３者が予測しにくい乱数を使用する。また、各種の自然現象や経済現象などのシミュレーションを行う場合その他、人為的でない自然で一様な一塊の数字を必要とする場合にも、乱数が用いられる。また、映像シーンの切り替えなどを行う映像処理装置においては、ランダムな色配列の連続画像を生成するために、乱数を適用することもある。

【０００４】図１には、一般的な乱数発生器２０の構成例を模式的に図解している。この乱数発生器２０は、カウンタ２１と、あらかじめ乱数テーブルを格納したＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）２２と、フリップ・フロップ２３とで構成される。すなわち、カウンタ２１は、クロック信号の入力に応答して逐次インクリメントされるカウント値を出力し、ＲＯＭ２２は入力されたカウント値に該当するテーブル・エントリの乱数を出力し、フリップ・フロップ２３は、クロック信号に同期して乱数を外部出力するようになっている。ＲＯＭ２２に格納される乱数テーブルは、例えばＭ系列（ｍａｘｉｍａｌ－ｐｅｒｉｏｄ　ｓｅｑｕｅｎｃｅ）乱数など各種の乱数発生方式等を用いて作成される。

【０００５】既に周知のように、乱数は、数字の列が不規則すなわち統計的精度で偏りがない一様性が充分保たれていることが好ましい。また、乱数は、再び同じ数字の列が繰り返されるようになるまでの周期が長いことが

好ましいとされている。

【０００６】ところが、図１に示すような構成の乱数発生器２０の場合．ＲＯＭ２２に格納されている乱数の個数が最終的に得られる乱数の周期となってしまう。したがって、長周期の乱数を得たい場合には、ＲＯＭ２２すなわち乱数テーブルの容量を大きくしなければならないことになり、コスト増大を招来してしまう。

【０００７】一般に、８ビットのＭ系列乱数を発生するハードウェア装置は、１ビットのシフト・レジスタを８個と．原始多項式に基づく演算を行うための排他的論理和装置（ＸＯＲ）とで構成される（図示しない）。Ｍ系列乱数によって生成される８ビットの擬似乱数の周期は．理論上、$2^8-1=255$となる。シフト・レジスタの個数を増やして周期を長くした場合、８ビットの擬似乱数を得るためにビット・マスクを施すと乱数性が失われるので、有効ではない。

【０００８】

【発明が解決しようとする課題】本発明の目的は．無作為に選ばれた全く不規則な数字の列で構成される乱数を発生することができる、優れた乱数発生装置及び乱数発生方法を提供することにある。

【０００９】本発明の更なる目的は．長周期の乱数を低コストで発生することができる、優れた乱数発生装置及び乱数発生方法を提供することにある。

【００１０】

【課題を解決するための手段】本発明は、上記課題を参酌してなされたものであり．その第１の側面は．第１の周期を持つ数列を生成する第１の数列生成部と．第２の周期を持つ数列を生成する第２の数列生成部と．前記第１及び第２の数列に対して所定の演算を適用する演算部と．前記演算部の演算結果を乱数として出力する出力部と．を具備することを特徴とする乱数発生装置である。

【００１１】前記第１の数列生成部は．カウント値を逐次インクリメントするカウンタと、第１の周期を持つ乱数テーブルを含み、前記乱数テーブル中からカウント値に該当するエントリの乱数を出力するようにしてもよい。

【００１２】また、前記第２の数列生成部は、０～（Ｎ－１）の数値の範囲を逐次インクリメントし、周期Ｎを有するカウンタであってもよい。あるいは、第２の数列生成部は、０～（Ｎ－１）の数値の範囲を階段状にインクリメントし．周期Ｎ×（Ｎ＋１）／２を有するカウンタであってもよい。

【００１３】また、前記演算部は、前記第１及び第２の数列に対してＸＯＲ（排他的論理和）又はＸＮＯＲ（排他的否定論理和）などの排他的論理演算を適用してもよい。排他的演算を施すことにより、出力が０又は１の一方に偏ることがなく、元の乱数の一様性を維持することができる。

【００１４】また、前記第１及び第２の周期は互いに約数を持たないような値に設定することによって．長周期化の効果を高めることができる。

【００１５】また、本発明の第２の側面は、第１の周期を持つ第１の数列を生成するステップと、第２の周期を持つ第２の数列を生成するステップと．前記第１及び第２の数列に対して所定の演算を適用するステップと、前記演算部の演算結果を乱数として出力するステップと、を具備することを特徴とする乱数発生方法である。

【００１６】前記第１の数列を生成するステップでは、第１の周期を持つ乱数テーブル中から．逐次インクリメントされるカウント値に該当するエントリの乱数を出力するようにしてもよい。

【００１７】また、前記第２の数列を生成するステップでは．０～（Ｎ－１）の数値の範囲を逐次インクリメントして、周期Ｎを持つカウント値を生成するようにしてもよい。あるいは、第２の数列を生成するステップでは．０～（Ｎ－１）の数値の範囲を階段状にインクリメントして、周期Ｎ×（Ｎ＋１）／２を有するカウント値を生成するようにしてもよい。

【００１８】また、前記所定の演算を適用するステップでは．前記第１及び第２の数列に対してＸＯＲ（排他的論理和）又はＸＮＯＲ（排他的否定論理和）などの排他的論理演算を適用するようにしてもよい。排他的演算を施すことにより．出力が０又は１の一方に偏ることがなく．元の乱数の一様性を維持することができる。

【００１９】また、前記第１及び第２の周期は互いに約数を持たないような値に設定することによって．長周期化の効果を高めることができる。

【００２０】

【作用】本発明に係る乱数発生装置は．第１の周期を持つ数列を生成する第１の数列生成部と．第２の周期を持つ数列を生成する第２の数列生成部と．前記第１及び第２の数列に対して所定の演算を適用する演算部とを備えている。

【００２１】第１の数列生成部は、例えば、乱数テーブルから読み出した乱数を出力する。また、第２の数列生成部は、通常のカウンタ出力である他．階段状その他複雑な形式でインクリメントするカウンタ出力、カウンタ出力でない数列などを出力する。

【００２２】演算部は、第１及び第２の数列に対してＸＯＲ（排他的論理和）やＸＮＯＲ（排他的否定論理和）などの排他的論理演算を適用して、偏りのない一様な乱数を生成することができる。

【００２３】生成された乱数は、第１及び第２の周期の最小公倍数を周期に持つので、容易に長周期化できる。

【００２４】本発明のさらに他の目的．特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００２５】

【発明の実施の形態】以下．図面を参照しながら本発明

の実施例を詳解する。

【００２６】図２には、本発明を実現した乱数発生器１０の構成を模式的に示している。同図に示すように、乱数発生器１０は、クロック信号に応答して逐次的に数列を出力する第１及び第２の数列生成部１１、１５と、各数列生成部１１及び１５の出力に対して所定の演算処理を適用する演算部１７と、該演算出力をクロックに同期して外部出力するフリップ・フロップ１８とで構成される。

【００２７】数列生成部１１及び１５は、それぞれＪ及びＫという周期で数列を生成するものとする。数列生成部１１又は１５のうちいずれか一方は、その出力自体が不規則で一様性のある乱数であることが好ましい。また、数列生成部１１又は１５の他方は、カウンタの出力＊又はカウンタ値に基づいた出力であってもよい。

【００２８】演算部１７は、数列生成部１１及び１５の出力同士に所定の論理演算を適用する機能モジュールである。ここで言う論理演算は、ＡＮＤやＯＲではなく、ＸＯＲ（排他的論理和）やＸＮＯＲ（排他的否定論理和）のような排他的論理演算であることが好ましい。これは、ＡＮＤでは出力が０に偏り、ＯＲでは出力が１に偏るのに対して、ＸＯＲやＸＮＯＲなどの排他的論理演算によれば、出力に偏りがないからである（［表１］を参照のこと）。すなわち、乱数に対してこのような排他的演算を適用しても、元の乱数の一様性は失われない。

【００２９】

【表１】

入力		AND	OR	XOR	XNOR
0	0	0	0	0	1
0	1	0	1	1	0
1	0	0	1	1	0
1	1	1	1	0	1

【００３０】演算部１７の出力、すなわち、この乱数発生器１０が出力する乱数は、各数列生成部１１及び１５が持つ周期Ｊ、Ｋの最小公倍数となる。したがって、周期Ｊ及びＫを適切な値に設定することにより、比較的短い周期Ｊしか持たない乱数を基にして、最長でＪ×Ｋという長周期を持つ乱数を生成することができる。

【００３１】図３には、本発明を実現した乱数発生器１０の他の構成例を図解している。同図に示す例では、数列生成部１１は、カウンタ１２とＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１３によって構成され、数列生成部１５は、カウンタ１６によって構成される。また、演算部１７は、ＸＯＲ（排他的論理和）によって構成される。

【００３２】カウンタ１２は、クロック信号の入力に応答して逐次インクリメントされるカウント値をＲＯＭ１３に供給する。ＲＯＭ１３には、あらかじめ乱数テーブルが格納されており、入力されたカウント値に該当するテーブル・エントリの乱数を出力するようになっている。乱数テーブルは、例えば、Ｍ系列（ｍａｘｉｍａｌ－ｐｅｒｉｏｄ ｓｅｑｕｅｎｃｅ）乱数など各種の乱数発生方式等を用いて作成することができる。

【００３３】この例では、ＲＯＭ１３には、２進数８ビットの値をとる乱数２５６個からなる乱数テーブルが格納されており、言い換えれば、数列生成部１１の周期は２５６である。

【００３４】なお、ＲＯＭ１３は、１チップ構成のメモリとして、乱数発生器１０に対して着脱・交換可能に構成することで、乱数テーブルを容易に更新することができる。あるいは、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）のような消去最書き込み可能なメモリをＲＯＭ１３に採用することによっても、乱数テーブルをプログラマブルにすることができる。

【００３５】また、カウンタ１６は、クロック信号の入力に応答して逐次インクリメントされるカウンタ値を基に、所定の数列を出力するように構成されている。

【００３６】乱数発生器１０を長周期化するという要請から、カウンタ１６の周期は、数列生成部１１の周期２５６との最小公倍数が大きくなる値に設定することが好ましい。この例では、カウンタ１６は、０から２４９までの値を０，１，０，１，２，０，１，２，３，０，１，２，３，…，０，１，２，…，２４９という具合に階段状にカウントしていくものとする。この場合のカウンタ１６の周期は２５０×２５１／２となる。したがって、乱数発生器１０全体の周期は２５６×２５０×２５１／２（＝８，０３２，０００）となり、数列生成部１１単体の乱数が持つ周期よりもはるかに長期化することができる。

【００３７】図３に示すような構成によれば、カウンタ１６やＲＯＭ１３の容量を変えることによって、用途に応じて充分な長さの周期を持つ乱数を発生させることができる。

【００３８】乱数発生器１０の最終的な周期は、ＲＯＭ１３すなわち乱数テーブルの容量とカウンタ１６の周期との最小公倍数となる。したがって、カウンタ１６の周期を、乱数の個数との約数のない値に設定することによって、長周期化の効果が高くなる。

【００３９】上述した例では、ＲＯＭ１３内の乱数の個数すなわち周期が２５６の場合に、カウンタ１６を０～２４９の間の値を階段状にカウントする構成にして、そ

の周期は２５０×２５１／２となる。この他、カウンタ１６を０～２４５，０～２４８，０～２５３の各値の間で階段状にカウントする場合であっても、周期はそれぞれ２４６×２４７／２，２４９×２５０／２，２５４×２５５／２となり、２５６とは約数がないので、長周期化の効果が高い。

【００４０】また、所望の周期の長さやコスト、ハードウェア設計上の制約などにより、カウンタ１６を、通常のカウンタ、上記よりもさらに複雑な階段状のカウント方式、あるいは、カウンタ以外の数列生成などの中から適宜選択することができる。

【００４１】上述の実施例では、図２及び図３に示すような専用のハードウェア装置を用いて乱数を発生する。勿論、プログラミング言語で記述されたコンピュータ・ソフトウェアなどを用いた所定の処理手順に従って、同様の乱数発生方式を実現することも可能である。

【００４２】図４には、本発明に係る乱数発生方式を実現するための処理手順をフローチャートの形式で図解している。以下、各ステップについて説明する。

【００４３】まず、ステップＳ１１では、所定の周期Ｊを持つ第１の数列を生成する。第１の数列は、それ自体が不規則で一様性のある乱数であることが好ましい。

【００４４】次いで、ステップＳ１２では、所定の周期Ｋを持つ第２の数列を生成する。第２の数列は、例えば、通常のカウンタの出力である他、階段状など複雑なインクリメントを行うカウンタ出力、あるいは、カウンタ出力ではない数列であってもよい。

【００４５】次いで、ステップＳ１３では、第１及び第２の数列同士に対して所定の演算を適用する。ここで言う演算は、論理演算を意味し、とりわけＸＯＲ（排他的論理和）やＸＮＯＲ（排他的否定論理和）などの排他的論理演算であることが好ましい。これは、ＡＮＤでは出力が０に偏り、ＯＲでは出力が１に偏るのに対して、ＸＯＲやＸＮＯＲなどの排他的論理演算によれば、出力に偏りがなくなるからである（前述及び［表１］を参照のこと）。

【００４６】最後に、ステップＳ１４において、上記の演算結果を乱数として出力して、この処理全体を終了する。

【００４７】上述した処理手順に従って生成される乱数は、第１及び第２の数列の各々が持つ周期Ｊ，Ｋの最小公倍数となる。したがって、周期Ｊ及びＫを適切な値に設定することにより、比較的短い周期Ｊしか持たない乱数を基にして、最大Ｊ×Ｋの長周期を持つ乱数を生成することができる。

【００４８】図５には、本発明に係る乱数発生方式を実現するための処理手順の他の例をフローチャートの形式で図解している。以下、各ステップについて説明する。

【００４９】まず、ステップＳ２１では、カウント値を出力し、次いでステップＳ２２では、所定の周期Ｊを持つ乱数テーブルの中からカウント値に該当するエントリから乱数を取り出す。乱数テーブルは、例えば、Ｍ系列（ｍａｘｉｍａｌ－ｐｅｒｉｏｄ　ｓｅｑｕｅｎｃｅ）乱数など各種の乱数発生方式等を用いて作成することができる。

【００５０】次いで、ステップＳ２３では、所定の周期Ｋを持つ数列を生成する。この数列は、例えば、通常のカウンタの出力である他、階段状など複雑なインクリメントを行うカウンタ出力、あるいは、カウンタ出力ではない数列であってもよい。

【００５１】次いで、ステップＳ２４では、ステップＳ２２で得られた乱数とステップＳ２３で生成された数列を各入力として、所定の演算を適用する。ここで言う演算は、論理演算を意味し、とりわけＸＯＲ（排他的論理和）やＸＮＯＲ（排他的否定論理和）などの排他的論理演算であることが好ましい。これは、ＡＮＤでは出力が０に偏り、ＯＲでは出力が１に偏るのに対して、ＸＯＲやＸＮＯＲなどの排他的論理演算によれば、出力に偏りがなくなるからである（前述及び［表１］を参照のこと）。

【００５２】最後に、ステップＳ２５において、演算結果を乱数として出力して、この処理全体を終了する。

【００５３】上述した処理手順に従って生成される乱数は、第１及び第２の数列の各々が持つ周期Ｊ，Ｋの最小公倍数となる。したがって、周期Ｊ及びＫを適切な値に設定することにより、比較的短い周期Ｊしか持たない乱数を基にして、最大Ｊ×Ｋの長周期を持つ乱数を生成することができる。

【００５４】［追補］以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【００５５】

【発明の効果】以上詳記したように、本発明によれば、無作為に選ばれた全く不規則な数字の列で構成される乱数を発生することができる、優れた乱数発生装置及び乱数発生方法を提供することができる。

【００５６】また、本発明によれば、長周期の乱数を低コストで発生することができる、優れた乱数発生装置及び乱数発生方法を提供することができる。

【００５７】本発明に係る乱数発生装置及び乱数発生方法によれば、ほぼ一様で偏りのない乱数を発生することができる。

【００５８】本発明に従って発生した乱数を、例えば、トレイル（ｔｒａｉｌ）などのシーン切り替え効果を行う映像処理装置に適用した場合には、色配列が美しい画

像を生成することができる。また、乱数の周期が非常に長いので、生成した画像を連続画像として見た際にも、視聴者は画像の繰り返しに気付くことがない。

【００５９】本発明に係る乱数発生装置によれば、ＲＯＭ１３に格納する乱数テーブルを書き換える、又は、別の乱数テーブルを持ったＲＯＭ１３に交換することによって、異なる乱数を容易に生成することができる。また、ＲＯＭ１３内の乱数の周期や、カウンタ１６の周期を切り替えることによって、様々な周期の乱数を生成することができる。

【００６０】また、本発明に係る乱数発生装置は、従来の方式に比し、コスト面、ハードウェア設計の面でも優れている。

【図面の簡単な説明】

【図１】一般的な乱数発生器２０の構成例（従来例）を模式的に示した図である。

【図２】本発明を実現した乱数発生器１０の構成を模式＊的に示した図である。

【図３】本発明を実現した乱数発生器１０の他の構成例を模式的に示した図である。

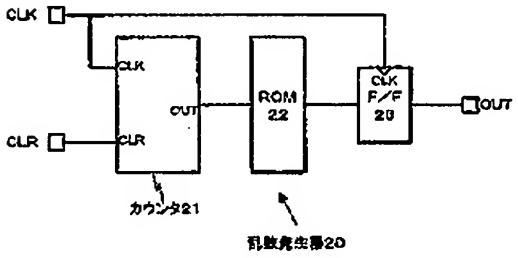
【図４】本発明に係る乱数発生方式を実現するための処理手順を示したフローチャートである。

【図５】本発明に係る乱数発生方式を実現するための処理手順の他の例を示したフローチャートである。

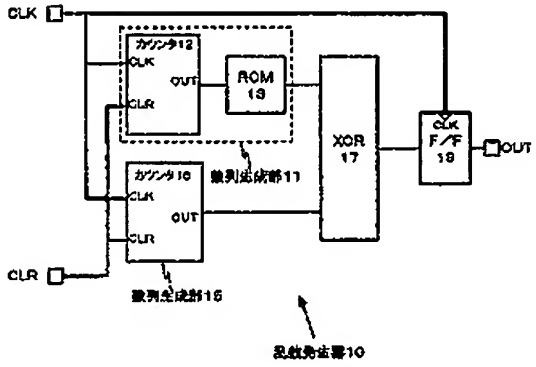
【符号の説明】

１０…乱数発生装置
１１…数列生成部
１２…カウンタ
１３…ＲＯＭ（乱数テーブル）
１５…数列生成部
１６…カウンタ
１７…演算部
１８…フリップ・フロップ

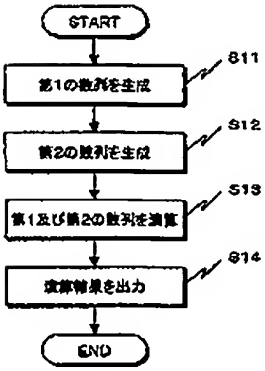
【図１】



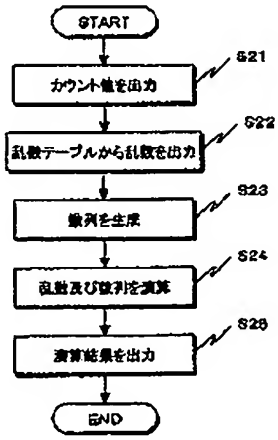
【図３】



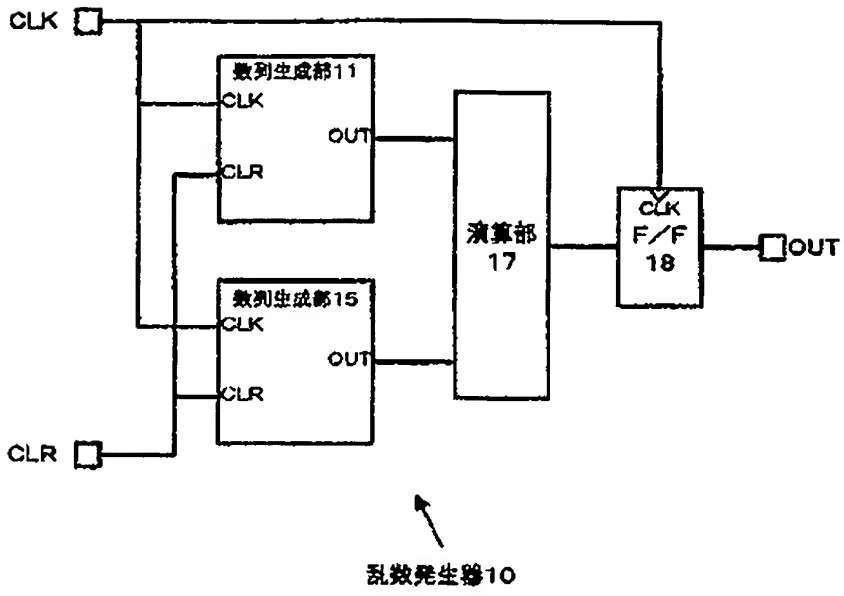
【図４】



【図５】



【図2】


CLK
数列生成部11
CLK
OUT
CLR
演算部
17
CLK
F/F
18
OUT
数列生成部15
CLK
OUT
CLR
CLR
乱数発生器10